Policy and Procedure on Research Subjects’ Right to Privacy

INTRODUCTION:
The privacy regulations (The Privacy Rule) that have been promulgated by the federal Office of Civil Rights under the Health Insurance Portability and Accountability Act (HIPAA) impact research involving human subjects. These regulations define conditions where certain health information may be used or disclosed in research activities. Further, the regulations define conditions where 'authorization' must be obtained from the patient. The full text of these regulations is available at www.hhs.gov/ocr/hipaa. Further mandates will follow once the upcoming security regulations are finalized.

DEFINITIONS PERTAINING TO PRIVACY IN RESEARCH:
♦ Health Information: any information, whether oral or recorded in any form or medium, that is created or received by an Upstate investigator, and relates to the past, present, or future physical or mental health or condition of an individual. To assist you in making the determination of what constitutes ‘health information’, this definition includes physical or mental information regarding the diagnosis, treatment and/or prevention of physical or mental conditions of the type that is now (or could be in the future) covered by health insurance.

♦ Individually identifiable health information (IIHI): is a subset of health information, including demographic information collected from an individual that identifies the individual (either directly, or through codes/identifiers).

♦ De-identified Health Information: health information can be considered de-identified if, EITHER:
  1. The investigator provides the Upstate IRB a written attestation by an expert in de-identification methods, that there is a very small risk that the information could be used by others to identify the subject.

  [The preamble to the Privacy Rule provides guidance (see, e.g., http://www.fcsr.gov/working-papers/wp22.html and http://www.fcsr.gov/docs/checklist__799.doc ) for what would be required in this regard, e.g., removing all direct identifiers, for reducing the number of variables on which a match might be made, and for limiting the distribution of records, etc.].

  OR

  2. The investigator certifies to the IRB (via the HIPAA De-identification Certification Form) that all of the following 18 identifiers are removed, and the investigator has no actual knowledge that the remaining information could be used, alone or in combination, to identify a specific subject. This is referred to as the Safe Harbor method. The 18 identifiers are name, address (street address, city, county, zip code - with certain exceptions), dates (e.g., birth date, admission date, discharge date, date of death) and individual ages if over 89, telephone #’s, fax #’s, electronic mail addresses, social security #’s, medical record numbers, health plan beneficiary #’s, account #’s,
certificate/license #'s, vehicle identifiers and serial #'s, medical device identifiers and serial #'s, Web Universal Resource Locators (URL's), Internet Protocol (IP) address #'s, Biometric identifiers (including finger and voice prints), full face photographic images and any comparable images, and any other unique identifying #, characteristic, or code.

♦ Use And Disclosure:
Use - sharing within the entity. For example, when members of the covered entity’s workforce share IIHI.
Disclosure - sharing outside the entity. For example, sharing IIHI with someone who is not a member of the covered entity’s workforce.

POLICY:
All Upstate investigators who conduct research where individually identifiable health information is used, generated, or disclosed are required to protect their research subjects’ right to privacy of their health information, using procedures as outlined in this document. This policy, and these procedures, are in addition to provisions already in place under the Common Rule at 45 CFR 46.

PROCEDURES:
The procedures below must be followed in addition to the IRB policies and Guidelines

A) Notice of Privacy Practice (NOPP):
Effective April 14, 2003, all subjects must be given a copy of the Upstate Notice of Privacy Practices (NOPP) at the time the consent/authorization form is signed. Their signing of the research consent form will acknowledge receipt of the NOPP.

B) Research involving De-identified data:
One of the methods described must be detailed for assuring that the data are de-identified. The HIPAA De-identification form, available on the IRB web site (http://www.upstate.edu/researchadmin/compliance/irb/), must be completed if the 18 listed identifiers are to be removed to satisfy HIPAA standards.

The Privacy Rule does not apply to:
1. De-identified information.
2. Coded information (all 18 identifiers must be either be coded or not used).
3. The code (link) that allows identification of coded information.

Note:
1. The code must not use any information from the 18 identifiers, such as initials, rearranged letters and/or numbers from name, birth date, etc.).
2. Even though the Privacy Rule does not apply to such coded information, the common rule considers coded information to be indirectly identifiable. Therefore, even if a researcher de-identifies information via coding, a protocol should be submitted to the IRB. The IRB will determine whether or not the research is covered by the common rule and/or the Privacy Rule.
C) Research Databases & Registries:

**Creating a Database/Registry that includes IIHI** – Databases and Registries created for future (unspecified) research are allowed under HIPAA. Depending on the circumstances, an authorization, a waiver of authorization or a data use agreement (if the information is in the form of a limited data set) will be required to assemble the data.

**Permissible uses for the Database/Registry** – Databases/registries may have multiple purposes. For research, the uses are regulated by the activities specified in the authorization, waiver of authorization, or data use agreement. Changes to the goals require new/amended authorizations, waivers, or data use agreements.

**Researcher access to the Database/Registry** – The researcher will need to obtain approval from the IRB to access the information for research purposes. Depending on the circumstances, an authorization, a waiver of authorization or a data use agreement (if the information is in the form of a limited data set) will be required to access the data.

D) Research Use Or Disclosure of IIHI Without Subject Authorization:

1. The IRB can waive the requirement to obtain authorization for use or disclosure of IIHI if one of the following conditions applies:

   a) The IRB finds and documents that all of the following criteria are addressed and met in the application submission (PI completes a waiver of authorization form):
      i) The use or disclosure of IIHI for the research involves no more than minimal risk to the privacy of individuals, based on:
         a. an adequate plan to protect identifiers from improper use
         b. an adequate plan to destroy identifiers at the earliest opportunity, and
         c. adequate written assurances that health information will be protected (e.g., not re-used/disclosed to any other person or entity except as required by law, for authorized oversight, etc.)
      ii) The research could not practicably be conducted without the waiver or alteration; and
      iii) The research could not be practicably be conducted without access to and use of the health information.

   b) The proposed use of health information is via a 'limited data set' (PI completes a limited data set form):
      A limited data set (LDS) contains information that is not completely de-identified. A LDS can contain dates of admission and discharge, dates of birth and death, dates of procedures, city, state, zip codes. A LDS must exclude the following direct identifiers: name, street address, telephone/fax numbers, e-mail address, social security number, certificate/license numbers, vehicle identifiers and serial numbers, uniform resource locators and internet protocol addresses, full face photographs and other comparable images, medical record numbers, account numbers, and health plan
numbers, device identifiers and serial numbers, biometric identifiers, including finger and voice print.

To use a Limited Data Set, a Data Use Agreement (DUA) must first be in place with the recipient of the information. The Data Use Agreement defines the permissible uses/disclosures of the LDS by the recipient, defines who can use or receive the data, and require the recipient to assure that data will not be re-identified and that individuals will not be contacted. The limited data set and data use agreement will be reviewed and executed by the Upstate Privacy Administrator. The PI should submit a limited data set (LDS) form to the IRB.

2. Minimum Necessary Requirement
The amount of information used, disclosed or requested must be limited to the minimum necessary to achieve the stated purpose. This requirement applies when authorization is not obtained.

3. Accounting for Disclosures Requirement
With the exception of limited data sets obtained under a data use agreement, disclosures of IIHI without authorization (i.e., a waiver of authorization was granted), made after April 14, 2003 require that:

All disclosures must be tracked.
When a subject requests an accounting of disclosures, s/he must be provided with a list of all individuals or entities to which their IIHI was disclosed without their authorization. The PI must keep track of each instance where s/he has provided an entity outside of Upstate Medical University with a subjects’ IIHI without that subject’s authorization on an Accounting Form (available on the IRB web site).

The research record must contain an Accounting Form for each subject and the researcher(s) must document any disclosures made for which authorization has not been obtained. The Accounting Form must be faxed to Clinical Data Services at 464-7781, after each entry.

In consideration of this accounting requirement, and the associated workload, it is strongly urged that the investigator either obtain an authorization, or utilize a limited data set prior to disclosure of his/her subjects’ IIHI.

E) Research Use of Health Information with Subject Authorization:
Under the HIPAA regulations, a patient coming into a doctor’s office or hospital for clinical treatment will sign consent, allowing the physician's office (or hospital, etc.) to use or disclose his or her health information for treatment, payment and health care operations purposes.

In the research setting, it is clear that health information could be generated and used or disclosed during the course of a research study. It is also clear that health information could be derived from research activities where the procedure involves a
simple blood draw from which genetic information can be obtained. It is thus important to assess the proposed research protocol for the need to access health information, and the potential for producing health information. If either is possible, then the HIPAA regulations will likely apply.

It is important to remember, that subjects can revoke their authorization for use of their health information at any time during the research. However, health information that was obtained prior to when authorization was revoked can continue to be used and disclosed if it's inclusion is important to maintain the integrity of the research study. For example, health information could be reported to account for a subject's withdrawal from the study, to be used as part of a marketing application to the FDA, to conduct investigations of scientific misconduct, or to report adverse events.

All research consent documents must include a section titled “Confidentiality of Records and Authorization to Use/Share Protected Health Information for Research”. This section (which replaces the section titled, “Confidentiality”) should be inserted as the last section in the consent, just prior to the signature section (see sample consent-[http://www.upstate.edu/researchadmin/irb/](http://www.upstate.edu/researchadmin/irb/)).

Follow the instructions (in italics) in attachment A to make the language study specific. In addition, the last section of the document (i.e., the signature section) must include additional language ([http://www.upstate.edu/researchadmin/irb/](http://www.upstate.edu/researchadmin/irb/-see attachment C (for adult subjects), D (for adult & minor subjects), and E (for minor subjects). Subjects must be given a signed copy of the consent/authorization form.

For studies which plan to “BANK” specimens for research, see [http://www.upstate.edu/researchadmin/irb/](http://www.upstate.edu/researchadmin/irb/-attachment B for appropriate language. If language from the sponsor is used, make sure the language requests permission to bank the specimens only, unless the future use can be specifically stated. The authorization for banking specimens cannot also serve as the authorization for future unknown uses of the specimens.

NOTE: If, during the course of the research, a disclosure of PHI is made for which authorization was not obtained, the researcher must record the disclosure on an Accounting Form (available on the IRB website). The form should be faxed to Clinical Data Services at 464-7781 and filed in the research record.

F) Retention of Records
The PI is required to retain all signed authorization forms (i.e., consent document which includes HIPAA language) for six years from the date signed by the subject (or subject’s representative) or from the date when last in effect, whichever is later.

Because there is no specific expiration date on the consent/authorization form, the current guidance is that the consent/authorization form should be kept indefinitely. Until there is further clarification, all consent/authorization forms should be kept indefinitely.
If the PI leaves Upstate, arrangements must be made to leave the consent/authorization forms with the Department. These arrangements should be communicated to the IRB office.

G) Policy Violations:
Upstate Medical University faculty, staff and students are obligated to report violations of this policy. Such reports will be brought before the privacy board at a convened meeting. The privacy board will make a determination, in consultation with applicable University Officials, to assess whether additional information and/or further investigation is required. The affected departmental Chair and Dean will be copied on all correspondence between the committee and the involved parties. Where violations are apparent, the Privacy officer, in consultation with applicable University Officials, may take immediate corrective action as deemed appropriate, prior to review by the full committee. In addition, other applicable University offices and/or external agencies (e.g., Office of Civil Rights) will be notified as required. **Note that health care providers who violate HIPAA may also be subject to significant criminal and civil penalties.**